

550001

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 10 月 7 日 (07.10.2004)

PCT

(10) 国際公開番号
WO 2004/086233 A1

- (51) 国際特許分類: G06F 12/14, G11B 20/10, H04L 9/08
- (21) 国際出願番号: PCT/JP2004/003579
- (22) 国際出願日: 2004 年 3 月 17 日 (17.03.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-085500 2003 年 3 月 26 日 (26.03.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 浅野 智之

(ASANO, Tomoyuki) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目1番7号 銀座ティークエイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

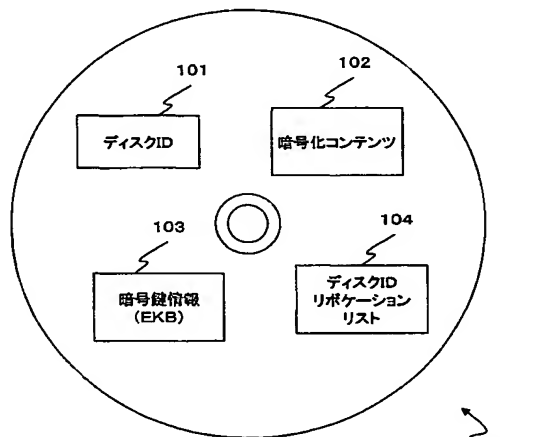
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL,

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING DEVICE, INFORMATION RECORDING MEDIUM MANUFACTURING DEVICE, AND METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラム



101...DISC ID
102...ENCRYPTED CONTENT
103...ENCRYPTION KEY INFORMATION (EKB)
104...DISC ID REVOCATION LIST

(57) Abstract: There are provided an information recording medium, an information processing device, and method capable of excluding flood and use of unauthorized copying of a content according to information recording medium management. An information recording medium containing an encrypted content stores an information recording medium ID as an identifier unique to the information recording medium and an information recording medium ID revocation list as a list of information recording medium ID's which have been judged to be unauthorized. An information processing device for reading out and reproducing a content stored in an information recording medium executes reproduction of a content only when the information recording medium ID stored in the information recording medium does not match with any of revoke information recording medium ID's described in the information recording medium ID revocation list. With this configuration, it is possible to exclude flood and use of unauthorized copying of a content.

[続葉有]

WO 2004/086233 A1



SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約: 情報記録媒体の管理に基づいてコンテンツの不正コピーの氾濫、利用を排除を実現した情報記録媒体、情報処理装置および方法を提供する。暗号化コンテンツを格納した情報記録媒体に、情報記録媒体固有の識別子である情報記録媒体IDと、不正であると判定された情報記録媒体IDのリストである情報記録媒体IDリポケーションリストとを格納し、情報記録媒体に格納されたコンテンツを読み出して再生する情報処理装置において、情報記録媒体に格納された情報記録媒体IDが、情報記録媒体IDリポケーションリストに記述されたりボーク情報記録媒体IDと一致しないことを条件としてコンテンツ再生処理を実行する構成とした。本構成により、コンテンツの不正コピーの氾濫、利用を排除することが可能となる。

明 細 書

情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びに
コンピュータ・プログラム

5

技術分野

本発明は、情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、CD、D
10 VD、MD等、各種のコンテンツ記録媒体に、記録媒体識別子を格納し、不正記録媒体のリストとしてのリボケーションリストに基づくコンテンツ利用制御を行うことにより、不正コピーコンテンツを格納したCD-Rディスク等の
氾濫、利用の防止を実現する情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムに関する。

15

背景技術

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウェアデータ（以下、これ
20 らをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはCD（Compact Disc）、DVD（Digital Versatile Disk）、MD（Mini Disk）等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、CDプレーヤ、DVDプレーヤ、MDプレーヤ等の再生装置、あるいはゲーム機器等
25 において再生され利用される。

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテ

ンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

特に、近年においては、情報をデジタル的に記録する記録装置や記憶媒体が普及しつつある。このようなデジタル記録装置および記憶媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができる。現実問題として、コンテンツをCD-R等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

このように、コピーが違法に行われた記憶媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。

発明の開示

本発明は、上述の問題点に鑑みてなされたものであり、コピーが違法に行われた記憶媒体からのコンテンツ再生、コンテンツ利用の実行を制限することを可能とした情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

本発明は、CD、DVD、MD等、各種のコンテンツ記録媒体に、記録媒体識別子を格納し、不正記録媒体のリストとしてのリボケーションリストに基づくコンテンツ利用制御を行うことにより、不正コピーコンテンツを格納したCD-R等の情報記録媒体の利用を制御することで、コピーが違法に行われた記憶媒体からのコンテンツ再生、コンテンツ利用の実行を制限することを可能とした情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

本発明の第 1 の側面は、

情報記録媒体であり、

暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

5 情報記録媒体固有の識別子である情報記録媒体 ID と、

不正であると判定された情報記録媒体 ID のリストである情報記録媒体 ID リボケーションリストと、

を格納したことを特徴とする情報記録媒体にある。

10 さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体 ID リボケーションリストは、該情報記録媒体 ID リボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成であることを特徴とする。

15 さらに、本発明の情報記録媒体の一実施態様において、前記暗号鍵情報は、前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キーブロック（EKB：Enabling Key Block）を含む構成であることを特徴とする。

20 さらに、本発明の情報記録媒体の一実施態様において、前記有効化キーブロック（EKB：Enabling Key Block）は、前記情報記録媒体の利用デバイスである情報処理装置に階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（DNK：Device Node Key）に基づいて復号処理の可能な暗号鍵情報であることを特徴とする。

25

さらに、本発明の第 2 の側面は、

コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、

不正であると判定された情報記録媒体 ID のリストである情報記録媒体 I

Dリボケーションリストを格納したメモリを有し、

情報記録媒体に格納された情報記録媒体IDと前記メモリに格納された情報記録媒体IDリボケーションリストに記述されたりボーク情報記録媒体IDとの照合処理を実行し、情報記録媒体に格納された情報記録媒体IDが、情報記録媒体IDリボケーションリストに記述されたりボーク情報記録媒体IDと一致しないことを条件としてコンテンツ再生処理を実行する構成を有することを特徴とする情報処理装置にある。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、
10 情報記録媒体に格納された情報記録媒体IDリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体IDリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体IDリボケーションリストのバージョンがメモリに格納した情報記録媒体IDリボケーションリストとのバージョンより新
15 しいものである場合に、情報記録媒体に格納された情報記録媒体IDリボケーションリストをメモリに格納するリスト更新処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、
20 階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（DNK：Device Node Key）を有し、前記情報記録媒体に格納された暗号化鍵情報としての有効化キープロック（EKB：Enabling Key Block）を前記デバイスノードキー（DNK：Device Node Key）に基づいて復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処
25 理を実行する構成であることを特徴とする。

さらに、本発明の第3の側面は、

情報記録媒体を製造する情報記録媒体製造装置であり、
暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

不正であると判定された情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストとを情報記録媒体に記録するとともに、

5 情報記録媒体固有の識別子である情報記録媒体 I D を製造する情報記録媒体毎に変更して記録する処理を実行する構成を有することを特徴とする情報記録媒体製造装置にある。

さらに、本発明の情報記録媒体製造装置の一実施態様において、前記情報記録媒体 I D リボケーションリストは、該情報記録媒体 I D リボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成である
10 ことを特徴とする。

さらに、本発明の情報記録媒体製造装置の一実施態様において、前記暗号鍵情報は、前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キープブロック（E K B : Enabling Key Block）を含む構成である
15 ことを特徴とする。

さらに、本発明の第 4 の側面は、

20 コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

情報記録媒体に格納された情報記録媒体 I D を読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と、前記情報記録媒体に格納された情報記録媒体 I D との照合処理を実
25 行するステップと、

情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とする情報処理方法にある。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、情報記録媒体に格納された情報記録媒体 ID リボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体 ID リボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体 ID リボケーションリストのバージョンがメモリに格納した情報記録媒体 ID リボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体 ID リボケーションリストをメモリに格納するリスト更新処理を実行するステップを有することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（DNK：Device Node Key）を適用して、前記情報記録媒体に格納された暗号化鍵情報としての有効化キープロック（EKB：Enabling Key Block）を復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処理を実行するステップを有することを特徴とする。

さらに、本発明の第 5 の側面は、
情報記録媒体を製造する情報記録媒体製造方法であり、
暗号化コンテンツと、前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、不正であると判定された情報記録媒体 ID のリストである情報記録媒体 ID リボケーションリストとを情報記録媒体に記録するステップと、
情報記録媒体固有の識別子である情報記録媒体 ID を製造する情報記録媒体毎に変更して記録する処理を実行するステップと、
を有することを特徴とする情報記録媒体製造方法にある。

さらに、本発明の第 6 の側面は、
コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する

コンピュータ・プログラムであり、

情報記録媒体に格納された情報記録媒体 I D を読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と、前記情報記録媒体に格納された情報記録媒体 I D との照合処理を実行するステップと、

5 情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行するステップと、

情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行するステップと、

10 を有することを特徴とするコンピュータ・プログラムにある。

本発明の構成に従えば、情報記録媒体に、暗号化コンテンツと、暗号化コンテンツの復号処理に必要とする暗号鍵情報と、情報記録媒体固有の識別子である情報記録媒体 I D と、不正であると判定された情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストとを格納した構成とし、情報記録媒体に格納されたコンテンツを読み出して再生する情報処理装置において、情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行する構成としたので、不正コピーコンテンツの格納媒体に記録された情報記録媒体 I D を情報記録媒体 I D リボケーションリストに記述することで、リスト化された I D を持つディスクの再生が防止され、コンテンツの不正コピーの氾濫、利用を排除することが可能となる。

また、本発明の構成では、情報処理装置において、情報記録媒体に格納された情報記録媒体 I D リボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体 I D リボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体 I D リボケーションリストのバージョンがメモリに格納した情報記録媒体 I D リボケーションリストとのバージョンより新しいものである場合に、情報

記録媒体に格納された情報記録媒体 I D リボケーションリストをメモリに格納するリスト更新処理を実行する構成としたので、随時更新されたリストによるコンテンツ再生制御の実行が可能となる。

- 5 なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、C D や F D、M O などの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供
10 することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

- 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細
15 書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

- 20 図 1 は、情報記録媒体の格納データについて説明する図である。
 図 2 は、情報記録媒体に格納される情報記録媒体（ディスク）I D リボケーションリスト（D I R L）のデータ構成を説明する図である。
 図 3 は、M A C 値生成処理例を示す図である。
 図 4 は、各種キー、データの暗号化処理、配布処理について説明するツリー
25 構成図である。
 図 5 は、各種キー、データの配布に使用される有効化キーブロック（E K B）の例を示す図である。
 図 6 は、コンテンツ鍵の有効化キーブロック（E K B）を使用した配布例と復号処理例を示す図である。

図 7 は、有効化キーブロック（E K B）のフォーマット例を示す図である。

図 8 は、有効化キーブロック（E K B）のタグの構成を説明する図である。

図 9 は、ツリー構成におけるカテゴリ分割を説明する図である。

図 1 0 は、ツリー構成におけるカテゴリ分割を説明する図である。

5 図 1 1 は、情報処理装置の構成を示すブロック図である。

図 1 2 は、情報処理装置の実行する処理を示すフローチャート図である。

図 1 3 は、情報処理装置の実行するリボーク判定処理を示すフローチャート図である。

10 図 1 4 は、情報処理装置の実行するコンテンツ再生処理を示すフローチャート図である。

図 1 5 は、情報記録媒体の製造および管理構成について説明する図である。

図 1 6 は、情報記録媒体製造装置の構成例を示す図である。

図 1 7 は、情報記録媒体の製造処理を示すフローチャート図である。

15

発明を実施するための最良の形態

以下、本発明の情報記録媒体、情報処理装置、および方法、並びにコンピュータ・プログラムについて詳細に説明する。

20

[1 . 情報記録媒体]

まず、図 1 以下を参照して、本発明に係る情報記録媒体のデータ記録構成例について説明する。図 1 は、C D (Compact Disc)、D V D (Digital Versatile Disk)、M D (Mini Disk) その他フラッシュメモリ等、各種の情報記録媒体 1 0
25 0 の格納データについて説明する図である。図 1 にはディスク状の媒体を例として示してあるが、本発明はディスク状の媒体に限らず、フラッシュメモリ等の各種の情報記録媒体において適用可能である。

情報記録媒体 1 0 0 には、図 1 に示す情報が格納されている。ディスク I D

101はディスク個別の識別子であり、消去や書き換えが困難であるように格納される。なお、以下に説明する実施例では、ディスク状の媒体をコンテンツ格納情報記録媒体の例として示しているの、その識別子をディスクIDとして説明する。フラッシュメモリ等の各種の情報記録媒体をコンテンツ格納情報記録媒体として利用した場合はディスクIDに対応する情報記録媒体IDが設定される。

暗号化コンテンツ102は暗号化されたコンテンツであり、暗号化コンテンツ102を復号するためのコンテンツ鍵は、例えば階層型キー配信構成によって、正当なコンテンツ利用機器としての情報処理装置に提供されるデバイスノードキー(DNK: Device Node Key)に基づいて、情報記録媒体100に格納された暗号鍵情報である有効化キーブロック(EKB: Enabling Key Block)103の復号処理等によってコンテンツ鍵を取得することができる。

15 階層型キー配信構成によるデバイスノードキー(DNK)の提供、およびデバイスノードキー(DNK)に基づく有効化キーブロック(EKB)の復号処理による鍵取得処理の詳細については後述する。

また、情報記録媒体100上にはディスクIDリボケーションリスト(DIRL: Disc ID Revocation List)104が格納される。ディスクIDリボケーションリスト(DIRL: Disc ID Revocation List)104は、不正コピー等が行われたと認定されたディスク、例えば市場に不正なコピーコンテンツを格納したCD-Rが発見された場合に、その不正CD-RにコンテンツとともにコピーされたディスクIDを抽出し、リスト化したデータである。ディスクIDリボケーションリスト(DIRL: Disc ID Revocation List)104の生成、管理、ディスク製造者に対するリスト情報提供は、特定の信頼される管理局(CA: Central Authority)が実行する。

ディスクIDリボケーションリスト(DIRL: Disc ID Revocation List)

のデータ構成について、図2を参照して説明する。ディスクIDリボケーションリスト(D I R L : Disc ID Revocation List) 150は、図2に示すように、ディスクIDリボケーションリスト(D I R L : Disc ID Revocation List)が作成された時期により単調増加するバージョン番号151と、排除すべきディスクのディスクIDを羅列したリボークディスクIDリスト152と、バージョン番号151とリボークディスクIDリスト152に対する改竄検証値153としての認証子が含まれる。改竄検証値153は、対象となるデータ、この場合はバージョン番号151とリボークディスクIDリスト152が改竄されているか否かを判別するために適用するデータであり、公開鍵暗号技術を用いたデジタル署名や、共通鍵暗号技術を用いたメッセージ認証コード(M A C : Message Authentication Code)が適用される。

改竄検証値153として公開鍵暗号技術を用いたデジタル署名を用いる際には、信頼できる機関、例えば上述の管理局(C A : Central Authority)の署名検証鍵(公開鍵)を再生機が取得し、管理局(C A : Central Authority)の署名生成鍵(秘密鍵)を用いて作られた署名を各再生機が取得した署名検証鍵(公開鍵)によって検証することで、バージョン番号151とリボークディスクIDリスト152が改竄されているか否かを判別する。

改竄検証値153としてメッセージ認証コード(M A C : Message Authentication Code)を用いた際のM A C生成、検証処理について、図3を参照して説明する。メッセージ認証コード(M A C : Message Authentication Code)は、データの改竄検証用のデータとして生成されるものであり、M A C生成処理、検証処理態様には様々な態様が可能であるが、1例としてD E S暗号処理構成を用いたM A C値生成例を図3に示す。

図3に示すように、対象となるメッセージ、この場合は、図2に示すバージョン番号151とリボークディスクIDリスト152を8バイト単位に分割し、(以下、分割されたメッセージをM1、M2、・・・、MNとする)、まず、

初期値 (Initial Value (以下、I Vとする)) とM 1を排他的論理和する (その結果をI 1とする)。次に、I 1をDES暗号化部に入れ、鍵 (以下、K 1とする) を用いて暗号化する (出力をE 1とする)。続けて、E 1およびM 2を排他的論理和し、その出力I 2をDES暗号化部へ入れ、鍵K 1を用いて暗号化する (出力E 2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたE Nがメッセージ認証符号 (MAC (Message Authentication Code)) となる。

MAC値は、その生成元データが変更されると、異なる値となり、検証対象のデータ (メッセージ) に基づいて生成したMACと、記録されているMACとの比較を行い、一致していれば、検証対象のデータ (メッセージ) は変更、改竄がなされていないことが証明される。

MAC生成における鍵K 1としては、たとえば、階層型キー配信構成によるデバイスノードキー (DNK) に基づく有効化キーブロック (EKB) の復号処理によって得られる鍵 (ルートキー) を適用することが可能である。また、初期値I Vとしては、予め定めた値を用いることが可能である。

[2. 階層型鍵配信ツリー構成]

次に、ブロードキャストエンクリプション (Broadcast Encryption) 方式の一態様である階層型鍵配信ツリー構成に従った鍵提供処理、再生機としての情報処理装置管理構成について説明する。

図4の最下段に示すナンバ0～15がコンテンツ利用を行なう情報処理装置としてのユーザデバイスである。すなわち図4に示す階層ツリー (木) 構造の各葉 (リーフ : leaf) がそれぞれのデバイスに相当する。

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図4に示す階層ツリー (木) 構造における自分のリーフからルートに至るまで

のノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスノードキー（DNK：Device Node Key））をメモリに格納する。図4の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKR（ルートキー）から、最下段から2番目の節（ノード）に記載されたキー：KR～K1111をノードキーとする。

図4に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図4のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

15

また、図4のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図4に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

20

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはCD等の情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵を送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払デー

25

5 タをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、
ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信
を行なうエンティティは、図4の点線で囲んだ部分、すなわちデバイス0, 1,
2, 3を1つのグループとして一括してデータを送付する処理を実行可能とな
る。このようなグループは、図4のツリー中に複数存在する。

10 なお、ノードキー、リーフキーは、ある1つの鍵管理センター機能を持つ管
理システムによって統括して管理してもよいし、各グループに対する様々なデ
ータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によ
ってグループごとに管理する構成としてもよい。これらのノードキー、リーフ
15 キーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管
理センター機能を持つ管理システム、プロバイダ、決済機関等が実行可能であ
る。

15 このツリー構造において、図4から明らかなように、1つのグループに含ま
れる3つのデバイス0, 1, 2, 3はデバイスノードキー(DNK: Device Node
Key)として共通のキーK00、K0、KRを含むデバイスノードキー(DN
K: Device Node Key)を保有する。このノードキー共有構成を利用すること
により、例えば共通のキーをデバイス0, 1, 2, 3のみに提供することが可
20 能となる。たとえば、共通に保有するノードキーK00は、デバイス0, 1,
2, 3に共通する保有キーとなる。また、新たなキーKnewをノードキーK
00で暗号化した値Enc(K00, Knew)を、ネットワークを介してあ
るいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0,
1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK0
25 0を用いて暗号Enc(K00, Knew)を解いて新たなキーKnewを得
ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号
化したデータであることを示す。

また、ある時点tにおいて、デバイス3の所有する鍵: K0011, K00

1, K 0 0, K 0, K Rが攻撃者（ハッカー）により解析されて露呈したことが
発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で
送受信されるデータを守るために、デバイス3をシステムから切り離す必要が
ある。そのためには、ノードキー：K 0 0 1, K 0 0, K 0, K Rをそれぞれ新
5 たな鍵K (t) 0 0 1, K (t) 0 0, K (t) 0, K (t) Rに更新し、デバ
イス0, 1, 2にその更新キーを伝える必要がある。ここで、K (t) a a a
は、鍵K a a aの世代（Generation）：tの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図5（A）に
10 示す有効化キーブロック（E K B：Enabling Key Block）と呼ばれるブロック
データによって構成されるテーブルをたとえばネットワーク、あるいは記録媒
体に格納してデバイス0, 1, 2に供給することによって実行される。なお、
有効化キーブロック（E K B）は、図4に示すようなツリー構造を構成する各
リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化
15 キーによって構成される。有効化キーブロック（E K B）は、キー更新プロ
ック（K R B：Key Renewal Block）と呼ばれることもある。

図5（A）に示す有効化キーブロック（E K B）には、ノードキーの更新の
必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構
20 成される。図5の例は、図4に示すツリー構造中のデバイス0, 1, 2におい
て、世代tの更新ノードキーを配布することを目的として形成されたブロック
データである。図4から明らかなように、デバイス0, デバイス1は、更新ノ
ードキーとしてK (t) 0 0, K (t) 0, K (t) Rが必要であり、デバイ
ス2は、更新ノードキーとしてK (t) 0 0 1, K (t) 0 0, K (t) 0,
25 K (t) Rが必要である。

図5（A）のE K Bに示されるようにE K Bには複数の暗号化キーが含まれ
る。最下段の暗号化キーは、E n c（K 0 0 1 0, K (t) 0 0 1）である。
これはデバイス2の持つリーフキーK 0 0 1 0によって暗号化された更新ノ

ードキー $K(t)001$ であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図 5 (A) の下から 2 段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー

5 $K(t)00$ を得ることができる。以下順次、図 5 (A) の上から 2 段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図 5 (A) の上から 1 段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要

10 なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス $K0000$ 、 $K0001$ は、図 5 (A) の上から 3 段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図 5 (A) の上から 2 段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図 5 (A) の上から 1 段目の暗号化キー $Enc(K(t)0,$

15 $K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 $K(t)R$ を得ることができる。なお、図 5 (A) のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図 4 に示すツリー構造の上位段のノードキー： $K(t)0$ 、 $K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図

20 5 (B) の有効化キーブロック (EKB) を用いることで、更新ノードキー $K(t)00$ をデバイス 0, 1, 2 に配布することができる。

図 5 (B) に示す EKB は、例えば特定のグループにおいて共有する新たな

25 コンテンツ鍵を配布する場合に利用可能である。具体例として、図 4 に点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のコンテンツ鍵 $K(t)con$ が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たな共通の更新コンテンツ鍵： $K(t)con$ を暗号化したデータ $Enc(K$

(t) 00, K(t) con) を図5 (B) に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

- 5 すなわち、デバイス0, 1, 2はEKBを処理して得たK(t) 00を用いて上記暗号文を復号すれば、t時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵K(t) conを得ることが可能になる。

- 10 図6に、t時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵K(t) conをEKBの処理によって取得する処理例を示す。EKBには、K(t) 00を用いてコンテンツ鍵K(t) conを暗号化したデータEnc(K(t) 00, K(t) con)と図5 (B) に示すデータとが格納されているとする。ここでは、デバイス0の処理例を示す。

- 15 図6に示すように、デバイス0は、記録媒体に格納されている世代:t時点のEKBと自分があらかじめ格納しているノードキーK000を用いて上述したと同様のEKB処理により、ノードキーK(t) 00を生成する。さらに、復号した更新ノードキーK(t) 00を用いて暗号化データEnc(K(t) 00, K(t) con)を復号して更新コンテンツ鍵K(t) conを取得する。
20 さらに、デバイスは、後にそれを使用するために自分だけが持つリーフキーK0000で暗号化して格納してもよい。

- 25 また、別の例として、ツリー構造のノードキーの更新は不必要で、時点tでのコンテンツ鍵K(t) conのみを必要な機器が得られればよい、という場合もある。この場合、下記のような方式とすることができる。

いま、図6の例と同様に、デバイス0, 1, 2にのみコンテンツ鍵K(t) conを送りたいとする。このとき、EKBは、
バージョン (Version): t

インデックス 暗号化キー

000 Enc (K000、K(t) con)

0010 Enc (K0010、K(t) con)

となる。

5

デバイス0、1はK000を用いて、またデバイス2はK0010を用いて上記EKBのうちの1つの暗号文を復号することによりコンテンツ鍵を得ることができる。このようにすることにより、ノードキーの更新は行えないものの、必要な機器にコンテンツ鍵を与える方法をより効率よく（すなわち、EKBに含まれる暗号文数を減らしてEKBのサイズを小さくするとともに、管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

10

図7に有効化キーブロック（EKB）のフォーマット例を示す。バージョン201は、有効化キーブロック（EKB）のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（EKB）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ203は、有効化キーブロック（EKB）中のデータ部の位置を示すポインタであり、タグポインタ204はタグ部の位置、署名ポインタ205は署名の位置を示すポインタである。

15

20

25

データ部206は、例えば更新するノードキーを暗号化したデータを格納する。例えば図5に示すような更新されたノードキーに関する各暗号化キー等を格納する。

タグ部207は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図8を用いて説明する。図8では、データとして先に図5（A）で説明した有効化キーブロック（E

KB)を送付する例を示している。この時のデータは、図8の表(b)に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図8の(a)に示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図8(c)に示すデータ列、およびタグ列が構成される。

タグは、データ $Enc(Kxxx, Kyyy)$ がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータ $Enc(Kxxx, Kyyy)...$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図5で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0: $Enc(K(t)0, K(t)root)$

00: $Enc(K(t)00, K(t)0)$

000: $Enc(K((t)000, K(T)00)$

...のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

図 7 に戻って、E K B フォーマットについてさらに説明する。署名 (Signature) 2 0 8 は、有効化キープブロック (E K B) を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。E K B を受領したデバイス 5 は署名検証によって正当な有効化キープブロック (E K B) 発行者が発行した有効化キープブロック (E K B) であることを確認する。

ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成 10 について、以下説明する。

図 9 に階層ツリー構造のカテゴリの分類の一例を示す。図 9 において、階層ツリー構造の最上段には、ルートキー K r o o t 3 0 1 が設定され、以下の中間段にはノードキー 3 0 2 が設定され、最下段には、リーフキー 3 0 3 が設定 15 される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

ここで、一例として最上段から第 M 段目のあるノードをカテゴリノード 3 0 4 として設定する。すなわち第 M 段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第 M 段の 1 つのノードを頂点として以下、M + 1 段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。 20

例えば図 9 の第 M 段目の 1 つのノード 3 0 5 にはカテゴリ A が設定され、このノード以下に連なるノード、リーフはカテゴリ A に区分され、様々なデバイスを含むカテゴリ A 専用のノードまたはリーフとして設定される。すなわち、ノード 3 0 5 以下を、カテゴリ A として区分されるデバイスの関連ノード、およびリーフの集合として定義する。 25

さらに、M段から数段分下位の段をサブカテゴリノード306として設定することができる。例えば図に示すようにカテゴリAノード305の2段下のノードに、カテゴリAに含まれるサブカテゴリAaノードとして、[再生専用器]のノードを設定する。さらに、サブカテゴリAaノードである再生専用器のノード306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる[PHS]ノード308と[携帯電話]ノード309を設定することができる。

- 10 さらに、カテゴリ、サブカテゴリは、デバイスの種類、メーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位で設定可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZにその
- 15 頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック(EKB)を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

20

- また、コンテンツプロバイダの管理するノードをカテゴリノードとした場合には、コンテンツプロバイダが提供するコンテンツを格納したCD、MD、DVD等の情報記録媒体またはネット配信コンテンツを利用する機器をカテゴリノード以下に設定して、その機器に対してその頂点ノード以下の下段のノードキー、リーフキーを提供することが可能となる。
- 25

このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノード

を管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック (EKB) を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

例えば、図 10 に示されるように、ツリー構成のシステムで、キー管理が行われる。図 10 の例では、 $8 + 2^4 + 3^2$ 段のノードがツリー構造とされ、ルートノードから下位の 8 段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばフラッシュメモリなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの 1 つのノードに、ライセンスを管理するシステムとして本システム (T システムと称する) が対応する。

すなわち、この T システムのノードよりさらに下の階層の 2^4 段のノードに対応するキーが、ショップサーバ、ライセンスサーバ等の管理エンティティとしてのサービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。この例の場合、これにより、 2^{24} (約 16 メガ) のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の 3^2 段の階層により、 2^{32} (約 4 ギガ) のユーザ (あるいはユーザデバイス) を規定することができる。最下段の 3^2 段のノードから T システムのノードまでのパス上の各ノードに対応するキーが、DNK (Device Node Key) を構成し、最下段のリーフに対応する ID がリーフ ID とされる。

例えば、コンテンツを暗号化したコンテンツ鍵は更新されたルートキー K_R' によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、EKB 内に配置される。EKB における末端から 1 つ上の段の更新ノードキーは EKB の末端のノードキーあるいはリーフキーによって暗号化され、EKB 内に配置される。

ユーザデバイスは、サービスデータに記述されているDNKのいずれかのキーを用いて、コンテンツデータとともに配布されるEKB内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、E

5 K B内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルートキーKR'を得ることができる。

上述したように、ツリーのカテゴリ分類により、1つのノードを頂点として、

10 以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化キーブロック(EKB)を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

15

[3 . 情報処理装置の処理]

次に、情報記録媒体に格納されたコンテンツの再生を実行するたとえば再生機等の情報処理装置におけるコンテンツ利用処理について説明する。

20 図11は、本発明を適用した情報処理装置500の一実施例構成を示すブロック図である。情報処理装置500は、入出力I/F(Interface)520、MPEG(Moving Picture Experts Group)等の各種符号化データの生成、復号を実行するコーデック530、A/D、D/Aコンバータ541を備えた入出力I/F(Interface)540、暗号処理手段550、ROM(Read Only Memory)

25 560、CPU(Central Processing Unit)570、メモリ580、記録媒体595の記録媒体インタフェース(I/F)590を有し、これらはバス510によって相互に接続されている。

入出力I/F520は、ネットワーク等、外部から供給されるデジタル信号

を受信し、バス 510 上に出力するとともに、バス 510 上のデジタル信号を受信し、外部に出力する。コーデック 530 は、バス 510 を介して供給される例えば M P E G 符号化されたデータをデコードし、入出力 I / F 540 に出力するとともに、入出力 I / F 540 から供給されるデジタル信号をエンコードしてバス 510 上に出力する。入出力 I / F 540 は、A / D, D / A コンバータ 541 を内蔵している。入出力 I / F 540 は、外部から供給されるアナログ信号を受信し、A / D, D / A コンバータ 541 で A / D (Analog Digital) 変換することで、デジタル信号として、コーデック 530 に出力するとともに、コーデック 530 からのデジタル信号を、A / D, D / A コンバータ 541 で D / A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

暗号処理手段 550 は、例えば、1 チップの L S I (Large Scale Integrated Curcuit) で構成され、バス 510 を介して供給される例えばコンテンツ等のデジタル信号を暗号化し、または復号し、バス 510 上に出力する構成を持つ。なお、暗号処理手段 550 は 1 チップ L S I に限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

R O M 560 は、例えば、情報処理装置ごとに固有の、あるいは複数の情報処理装置のグループごとに固有のデバイスキーであるリーフキーと、複数の情報処理装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。C P U 570 は、メモリ 580 に記憶されたプログラムを実行することで、コーデック 530 や暗号処理手段 550 等を制御する。

メモリ 580 は、上述したディスク I D リボケーションリスト (D I R L : Disc ID Revocation List) をディスクから読み取り格納する。ディスク I D リボケーションリスト (D I R L) はセキュアにメモリに格納する。例えば情報処理装置 500 に設定された I D に基づく暗号化を施してメモリに格納するなどにより耐タンパ性を保持したデータとして格納することが好ましい。

このようにディスク I D リボケーションリスト (D I R L) は外部から消されたり、内容を改ざんされたり、古いバージョンのリストに入れ替えられることを容易に実行されないように格納する。

- 5 メモリ 5 8 0 には、さらに、CPU 5 7 0 が実行するプログラムや、CPU 5 7 0 の動作上必要なデータを記憶する領域も含まれる。記録媒体インタフェース 5 9 0 は、デジタルデータを記録再生可能な記録媒体 5 9 5 を駆動することにより、記録媒体 5 9 5 からデジタルデータを読み出し (再生し)、バス 5 1 0 上に出力するとともに、バス 5 1 0 を介して供給されるデジタルデータを、
- 10 記録媒体 5 9 5 に供給して記録させる。

- 記録媒体 5 9 5 は、例えば、DVD、CD、MD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、記録媒体インタフェース 5 9 0 に対して着脱可能な構成であるとする。但し、記録媒体 5 9 5 は、情報処理装置 5 0 0 に内蔵する構成としてもよい。
- 15

情報処理装置 5 0 0 における情報記録媒体格納コンテンツの利用処理について、図 1 2 ~ 図 1 4 のフローを参照して説明する。

20

図 1 2 は、情報処理装置に図 1 を参照して説明した情報記録媒体をセットし、コンテンツ再生を開始する際に事前処理として実行される処理である。

- ステップ S 1 0 1 において、情報処理装置は、情報記録媒体に格納されたディスク I D リボケーションリスト (D I R L) を読み取り、正当性、すなわち改竄の有無の判定処理を行う。これは、前述したように、ディスク I D リボケーションリスト (D I R L) の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵 (公開鍵) によって検証する。また、改竄検証値としてメッセージ認証コード (M A C : Message Authentication
- 25

Code) が付与されている場合は、先に図 3 を参照して説明した M A C 検証処理が実行される。

5 ディスク I D リボケーションリスト (D I R L) に改竄があると判定 (ステップ S 1 0 2 : N o) されると、ステップ S 1 0 6 に進み、その後の処理、すなわちコンテンツ再生を行うことなく処理を終了する。

10 ディスク I D リボケーションリスト (D I R L) に改竄がないと判定 (ステップ S 1 0 2 : Y e s) されると、ステップ S 1 0 3 に進み、情報記録媒体から読み出したディスク I D リボケーションリスト (D I R L) のバージョンと、情報処理装置のメモリに格納されているディスク I D リボケーションリスト (D I R L) とのバージョン比較を実行する。情報記録媒体から読み出したディスク I D リボケーションリスト (D I R L) のバージョンが情報処理装置に格納されているディスク I D リボケーションリスト (D I R L) より新しい場合は、ステップ S 1 0 5 において、情報処理装置のメモリに情報記録媒体から読み出したディスク I D リボケーションリスト (D I R L) を書き込み、更新する。この処理により、情報処理装置のメモリには随時更新されたディスク I D リボケーションリスト (D I R L) が格納される。

20 なお、情報処理装置のメモリにディスク I D リボケーションリスト (D I R L) が未格納の場合には、バージョン比較を行うことなく、改竄検証のみを行い正当性の確認された情報記録媒体から読み出したディスク I D リボケーションリスト (D I R L) を情報処理装置のメモリに書き込む処理を実行する。

25 なお、上述した例では、ディスク上にディスク I D リボケーションリスト (D I R L) が格納されていて、それを用いて再生機のメモリのディスク I D リボケーションリスト (D I R L) を更新する例を説明したが、情報処理装置が電話回線やインターネット経由で管理局またはそこから委託されたサーバから最新のディスク I D リボケーションリスト (D I R L) を入手して更新しても

よいし、情報処理装置が製造される際に、その時点での最新のディスクIDリボケーションリスト(DIRL)をメモリに格納するようにしてもよい。また、たとえば家庭内でネットワークを構成している機器同士で互いに格納するディスクIDリボケーションリスト(DIRL)のバージョンを教えあい、新しいものを用いて古いものを更新するようにしてもよい。さらに、メディアが書き込み可能なメディアであれば、記録機器が最新バージョンのディスクIDリボケーションリスト(DIRL)を書き込み、それを用いてそのメディアを扱った機器のディスクIDリボケーションリスト(DIRL)を更新するようにしてもよい。

10

次に、図13を参照して、情報処理装置が実行するリボーク判定処理について説明する。この処理は、図12の処理に続いて実行する。ステップS201において、情報処理装置は、情報記録媒体から情報記録媒体IDを読み出す。

15 ステップS202において、情報処理装置のメモリに格納したディスクIDリボケーションリスト(DIRL)のリボークIDリストと情報記録媒体から読み出した情報記録媒体IDとの照合処理を実行する。

20 ステップS203において、ディスクIDリボケーションリスト(DIRL)のリボークIDリストと情報記録媒体から読み出した情報記録媒体IDとが一致した場合は、ステップS204に進み、その後の処理、すなわちコンテンツ再生処理を実行することなく処理を終了する。

25 リボークIDリストと情報記録媒体から読み出した情報記録媒体IDとが一致した場合は、上述の管理局(CA: Central Authority)が、不正流通CD-R等に基づいてコピーされた情報記録媒体IDを抽出し、リボークIDリストにその情報記録媒体IDを記述したものであることを意味する。従って、情報処理装置にセットされた情報記録媒体は、不正流通CD-R等であり、既に正当なコンテンツ利用権が失われた情報記録媒体またはそのコピーであり、

情報処理装置は、この情報記録媒体からのコンテンツ再生を実行することなく処理を終了する。

5 ステップS203において、ディスクIDリボケーションリスト(DIRL)の
リボークIDリストと情報記録媒体から読み出した情報記録媒体IDとが一致しなかった場合は、コンテンツ再生処理に移行する。

10 図14を参照してコンテンツ再生処理シーケンスについて説明する。ステップS301において、情報処理装置は、情報記録媒体から、暗号鍵情報、すな
わち有効化キーブロック(EKB)を読み出す。ステップS302において、
情報処理装置は、階層型キー配信構成によって予め情報処理装置に提供されて
いるデバイスノードキー(DNK)に基づいて有効化キーブロック(EKB)
の復号処理を実行して、コンテンツ鍵を取得する。この処理手順は、先に図6
を参照して説明したとおりである。

15

ステップS303では、情報記録媒体から再生対象の暗号化コンテンツを読み出して、ステップS302で取得したコンテンツ鍵を用いてステップS304において復号し、再生する。ステップS305において、再生対象コンテンツがさらにある場合は、ステップS303, 304の処理を繰り返し実行し、
20 再生対象コンテンツが終了すると処理を終了する。

25 なお、また、コンテンツ鍵を導出する際に、EKBだけでなく、ディスク上に記録されている他の情報、たとえば、コンテンツのコピー制御情報などを適用してコンテンツ鍵を導出する構成としてもよい。また、ディスク製造業者が
ディスク製造時に、ディスク上に、ルートキーで暗号化したコンテンツ鍵を格納しておき、情報処理装置はこれを復号してコンテンツ鍵を得るようにしてもよい。

また、同一の情報記録媒体で、たとえばコンテンツが格納されているアドレ

スにより別個のコンテンツ鍵を用いてコンテンツを暗号化した構成も可能であり、この場合は、情報処理装置において、ステップS 3 0 1～S 3 0 4のコンテンツ鍵の導出、コンテンツの読み出し・復号を必要なだけ繰り返し実行する。

5

[4 . 情報記録媒体の製造、提供、管理構成]

次に、コンテンツを記録した情報記録媒体の製造、提供、管理構成について、図 1 5 を参照して説明する。

10 図 1 5 に示す例では、情報記録媒体製造業者 6 0 3 において、CD等の情報記録媒体 6 0 4 が製造されユーザの情報処理装置 6 0 5 において利用される。

図 1 を参照して説明したように、情報記録媒体には、暗号化コンテンツ、暗号鍵情報、情報記録媒体（ディスク）ID、情報記録媒体（ディスク）IDリボケーションリスト（DIRL）とが格納される。

コンテンツプロバイダ 6 0 2 は、コンテンツを暗号化し、暗号化コンテンツとして情報記録媒体製造業者 6 0 3 に提供する。さらに、特定のユーザの持つデバイス（情報処理装置）の持つデバイスノードキー（DNK）においてのみ
20 処理可能な有効化キープブロック（EKB）を情報記録媒体製造業者 6 0 3 に提供する。管理局（CA：Central Authority）6 0 1 は、情報記録媒体（ディスク）IDおよび、情報記録媒体（ディスク）IDリボケーションリスト（DIRL）を情報記録媒体製造業者 6 0 3 に提供する。

25 情報記録媒体製造業者 6 0 3 は、コンテンツプロバイダ 6 0 2 から受領した暗号化コンテンツおよび有効化キープブロック（EKB）と、管理局（CA：Central Authority）6 0 1 から受領した情報記録媒体（ディスク）IDおよび、情報記録媒体（ディスク）IDリボケーションリスト（DIRL）を情報記録媒体に格納し情報記録媒体（ディスク）6 0 4 を製造し、ユーザに提供す

る。ユーザは情報記録媒体（ディスク）604を情報処理装置605にセットして上述したコンテンツ利用処理を行う。

5 なお、デバイスノードキー(DNK)のユーザ情報処理装置に対する提供は、
管理局601またはコンテンツプロバイダ602のいずれが行ってもよい。あるいは図示しない他のサービスプロバイダが行ってもよい。

10 情報記録媒体製造装置の構成例について、図16を参照して説明する。情報記録媒体製造装置700は、入出力I/F(Interface)720、暗号処理手段750、ROM(Read Only Memory)760、CPU(Central Processing Unit)770、メモリ780、記録媒体795の記録媒体インタフェース(I/F)790を有し、これらはバス710によって相互に接続されている。

15 入出力I/F720は、外部から供給されるデジタル信号を受信し、バス710上に出力する。例えばコンテンツプロバイダからの暗号化コンテンツ、有効化キープブロック(EKB)、および管理局(CA: Central Authority)から受領する情報記録媒体(ディスク)IDおよび、情報記録媒体(ディスク)IDリボケーションリスト(DIRL)などのデータをネットワークを介して受信することができる。なお、情報記録媒体(ディスク)IDは、製造するディスクの数に応じた数のIDを管理局(CA: Central Authority)から受領する。
20

25 暗号処理手段730は、例えば、1チップのLSI(Large Scale Integrated Circuit)で構成され、バス710を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス710上に出力する構成を持つ。コンテンツプロバイダから提供されるコンテンツが暗号化コンテンツでない場合には、暗号処理手段730において暗号化する。なお、暗号処理手段750は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

メモリ 740 は、コンテンツプロバイダから受領した暗号化コンテンツおよび有効化キーブロック (EKB) と、管理局 (CA: Central Authority) から受領した情報記録媒体 (ディスク) ID および、情報記録媒体 (ディスク) ID リボケーションリスト (DIRL) とを格納する。なお、情報記録媒体 (ディスク) ID は、製造するディスクの数に応じた数の ID を管理局 (CA: Central Authority) から受領しメモリ 740 に格納する。

コントローラ 750 は、情報記録媒体の製造プログラムに従った制御を実行する。CPU 等の制御部およびプログラム格納メモリを有する。コントローラ 750 の制御にしたがって、メモリ 740 に格納されたデータが、記録媒体に格納される。

記録媒体 770 は、例えば、DVD、CD、MD 等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいは RAM 等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、記録媒体インタフェース 760 から記録データが供給されて記録格納される。

ディスクの製造処理手順について図 17 を参照して説明する。図 17 の処理は、情報記録媒体製造業者の情報記録媒体製造装置において実行する処理である。情報記録媒体製造装置には、上述したようにメモリが備えられ、メモリにコンテンツプロバイダから受領した暗号化コンテンツおよび有効化キーブロック (EKB) と、管理局 (CA: Central Authority) から受領した情報記録媒体 (ディスク) ID および、情報記録媒体 (ディスク) ID リボケーションリスト (DIRL) とが格納されているものとする。なお、情報記録媒体 (ディスク) ID は、製造するディスクの数に応じた数の ID を管理局 (CA: Central Authority) から受領する。

ステップ S401 において、管理局 (CA: Central Authority) から受領

し、メモリに格納済みの情報記録媒体（ディスク）IDリボケーションリスト（DIRL）をメモリから読み出し、ステップS402、ステップS403において、コンテンツプロバイダから受領した有効化キープブロック（EKB）、暗号化コンテンツをメモリから読み出し、ステップS404において、これらの情報を情報記録媒体（ディスク）に書き込んでマスターディスクを製造する。

次に、ステップS405において、マスターディスクに基づくスタンプによるスタンプ処理により、複製としてのディスクを製造する。次に、ステップS406において、管理局（CA：Central Authority）から受領し、メモリに格納済みの、ディスクIDを順次取り出してディスクに書き込む。ステップS407において、製造枚数が、管理局（CA：Central Authority）から受領したディスクID数に達した場合は、その時点でディスク製造を終了する。

このように、ディスク製造業者は、管理局（CA：Central Authority）から受領したディスクIDの数に応じて、それぞれの製造ディスクに異なるIDを格納する。

従って、市場に流通する情報記録媒体（ディスク）にはそれぞれ異なるIDが設定されていることになり、同一のディスクIDが設定されている複数のディスクが発見された場合は、不正なコピーが実行されているものと判断し、管理局（CA：Central Authority）が情報記録媒体（ディスク）IDリボケーションリスト（DIRL）にそのディスクIDを書き込む更新処理を実行し、更新されたリストがディスク製造業者に提供され、新規ディスクには、そのリストが格納される。

25

更新リストを持つディスクを購入したユーザが、情報処理装置にディスクをセットし、コンテンツ再生処理を実行する際には、前述したように、情報処理装置内のメモリに格納された情報記録媒体（ディスク）IDリボケーションリスト（DIRL）とのバージョン比較が実行され、更新されたリストがメモリ

に格納される。従って、ユーザの情報処理装置のメモリに格納されるリストは、随時更新される。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

5 なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

10 例えば、プログラムは記憶媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

25 なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体に

インストールすることができる。

5 なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

産業上の利用可能性

10 以上、説明したように、本発明の構成によれば、情報記録媒体に、暗号化コンテンツと、暗号化コンテンツの復号処理に必要とする暗号鍵情報と、情報記録媒体固有の識別子である情報記録媒体IDと、不正であると判定された情報記録媒体IDのリストである情報記録媒体IDリボケーションリストとを格納した構成とし、情報記録媒体に格納されたコンテンツを読み出して再生する
15 情報処理装置において、情報記録媒体に格納された情報記録媒体IDが、情報記録媒体IDリボケーションリストに記述されたリボーク情報記録媒体IDと一致しないことを条件としてコンテンツ再生処理を実行する構成としたので、不正コピーコンテンツの格納媒体に記録された情報記録媒体IDを情報記録媒体IDリボケーションリストに記述することで、リスト化されたIDを持つディスクの再生が防止され、コンテンツの不正コピーの氾濫、利用を排除す
20 ることが可能となる。

 また、本発明の構成では、情報処理装置において、情報記録媒体に格納された情報記録媒体IDリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体IDリボケーション
25 リストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体IDリボケーションリストのバージョンがメモリに格納した情報記録媒体IDリボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体IDリボケーションリストをメモリに格納するリスト更新処理を実行する構成としたので、随時更新されたリストによ

るコンテンツ再生制御の実行が可能となる。

請求の範囲

1. 情報記録媒体であり、
5 暗号化コンテンツと、
前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、
情報記録媒体固有の識別子である情報記録媒体 I D と、
不正であると判定された情報記録媒体 I D のリストである情報記録媒体 I
D リボケーションリストと、
10 を格納したことを特徴とする情報記録媒体。
2. 前記情報記録媒体 I D リボケーションリストは、
該情報記録媒体 I D リボケーションリストの格納データの改竄の有無を判
定するための改竄検証値を持つ構成であることを特徴とする請求項 1 に記載
15 の情報記録媒体。
3. 前記暗号鍵情報は、
前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データと
しての有効化キーブロック (E K B : Enabling Key Block) を含む構成である
20 ことを特徴とする請求項 1 に記載の情報記録媒体。
4. 前記有効化キーブロック (E K B : Enabling Key Block) は、
前記情報記録媒体の利用デバイスである情報処理装置に階層型鍵配信ツリ
ー構成を適用して提供された鍵情報としてのデバイスノードキー (D N K :
25 Device Node Key) に基づいて復号処理の可能な暗号鍵情報であることを特徴
とする請求項 3 に記載の情報記録媒体。
5. コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行
する情報処理装置であり、

不正であると判定された情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストを格納したメモリを有し、

- 5 情報記録媒体に格納された情報記録媒体 I D と前記メモリに格納された情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D との照合処理を実行し、情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行する構成を有することを特徴とする情報処理装置。

10 6. 前記情報処理装置は、

- 15 情報記録媒体に格納された情報記録媒体 I D リボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体 I D リボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体 I D リボケーションリストのバージョンがメモリに格納した情報記録媒体 I D リボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体 I D リボケーションリストをメモリに格納するリスト更新処理を実行する構成であることを特徴とする請求項 5 に記載の情報処理装置。

20 7. 前記情報処理装置は、

階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー (DNK : Device Node Key) を有し、

- 25 前記情報記録媒体に格納された暗号化鍵情報としての有効化キーブロック (EKB : Enabling Key Block) を前記デバイスノードキー (DNK : Device Node Key) に基づいて復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処理を実行する構成であることを特徴とする請求項 5 に記載の情報処理装置。

8. 情報記録媒体を製造する情報記録媒体製造装置であり、

暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

不正であると判定された情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストとを情報記録媒体に記録するとともに、

- 5 情報記録媒体固有の識別子である情報記録媒体 I D を製造する情報記録媒体毎に変更して記録する処理を実行する構成を有することを特徴とする情報記録媒体製造装置。

9. 前記情報記録媒体 I D リボケーションリストは、

- 10 該情報記録媒体 I D リボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成であることを特徴とする請求項 8 に記載の情報記録媒体製造装置。

10. 前記暗号鍵情報は、

- 15 前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キープブロック (E K B : Enabling Key Block) を含む構成であることを特徴とする請求項 8 に記載の情報記録媒体製造装置。

- 20 11. コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

情報記録媒体に格納された情報記録媒体 I D を読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストに記述されたリボーク情報記録媒体 I D と、前記情報記録媒体に格納された情報記録媒体 I D との照合処理を実

- 25 行するステップと、

情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたリボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とする情報処理方法。

1 2. 前記情報処理方法は、さらに、

情報記録媒体に格納された情報記録媒体 I D リボケーションリストの改竄
検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情
5 報記録媒体 I D リボケーションリストとのバージョン比較を実行し、情報記録
媒体に格納された情報記録媒体 I D リボケーションリストのバージョンがメ
モリに格納した情報記録媒体 I D リボケーションリストとのバージョンより
新しいものである場合に、情報記録媒体に格納された情報記録媒体 I D リボケ
ーションリストをメモリに格納するリスト更新処理を実行するステップを有
10 することを特徴とする請求項 1 1 に記載の情報処理方法。

1 3. 前記情報処理方法は、さらに、

階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノ
ードキー (DNK : Device Node Key) を適用して、前記情報記録媒体に格納
15 された暗号化鍵情報としての有効化キーブロック (EKB : Enabling Key
Block) を復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に
適用する鍵の取得処理を実行するステップを有することを特徴とする請求項
1 1 に記載の情報処理方法。

20 1 4. 情報記録媒体を製造する情報記録媒体製造方法であり、

暗号化コンテンツと、前記暗号化コンテンツの復号処理に必要なとする暗号鍵
情報と、不正であると判定された情報記録媒体 I D のリストである情報記録媒
体 I D リボケーションリストとを情報記録媒体に記録するステップと、

情報記録媒体固有の識別子である情報記録媒体 I D を製造する情報記録媒
25 体毎に変更して記録する処理を実行するステップと、
を有することを特徴とする情報記録媒体製造方法。

1 5. コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実
行するコンピュータ・プログラムであり、

情報記録媒体に格納された情報記録媒体 I D を読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体 I D のリストである情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と、前記情報記録媒体に格納された情報記録媒体 I D との照合処理を実

5 行するステップと、

情報記録媒体に格納された情報記録媒体 I D が、情報記録媒体 I D リボケーションリストに記述されたりボーク情報記録媒体 I D と一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

1/17

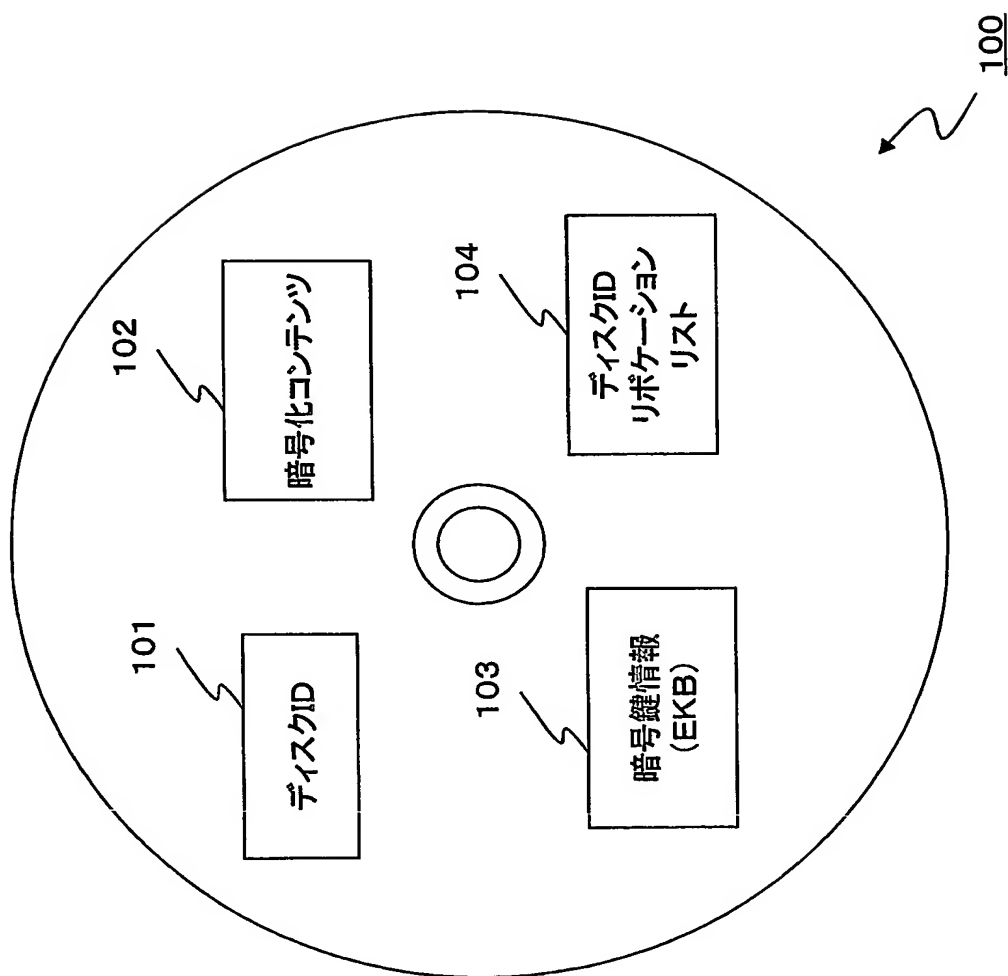


Fig. 1

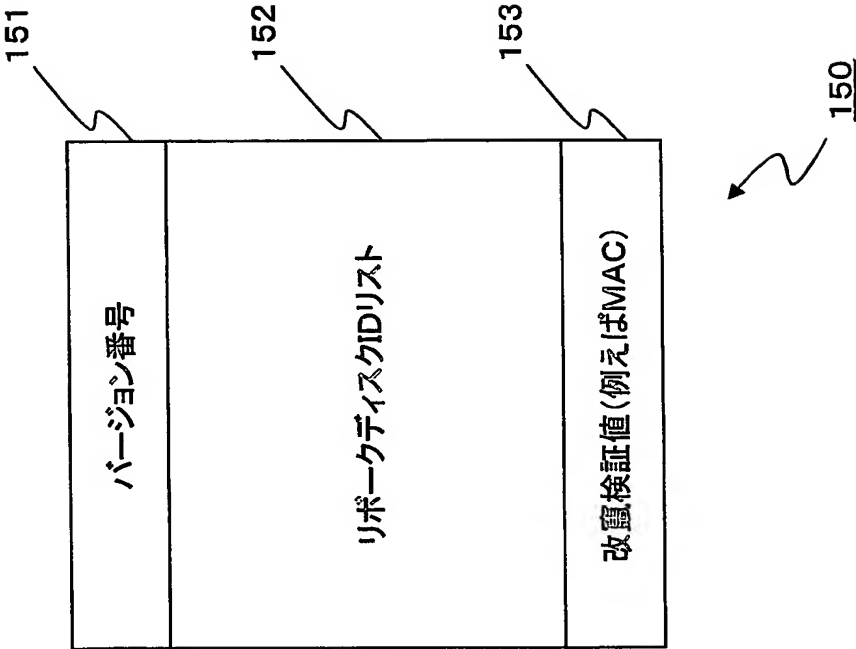
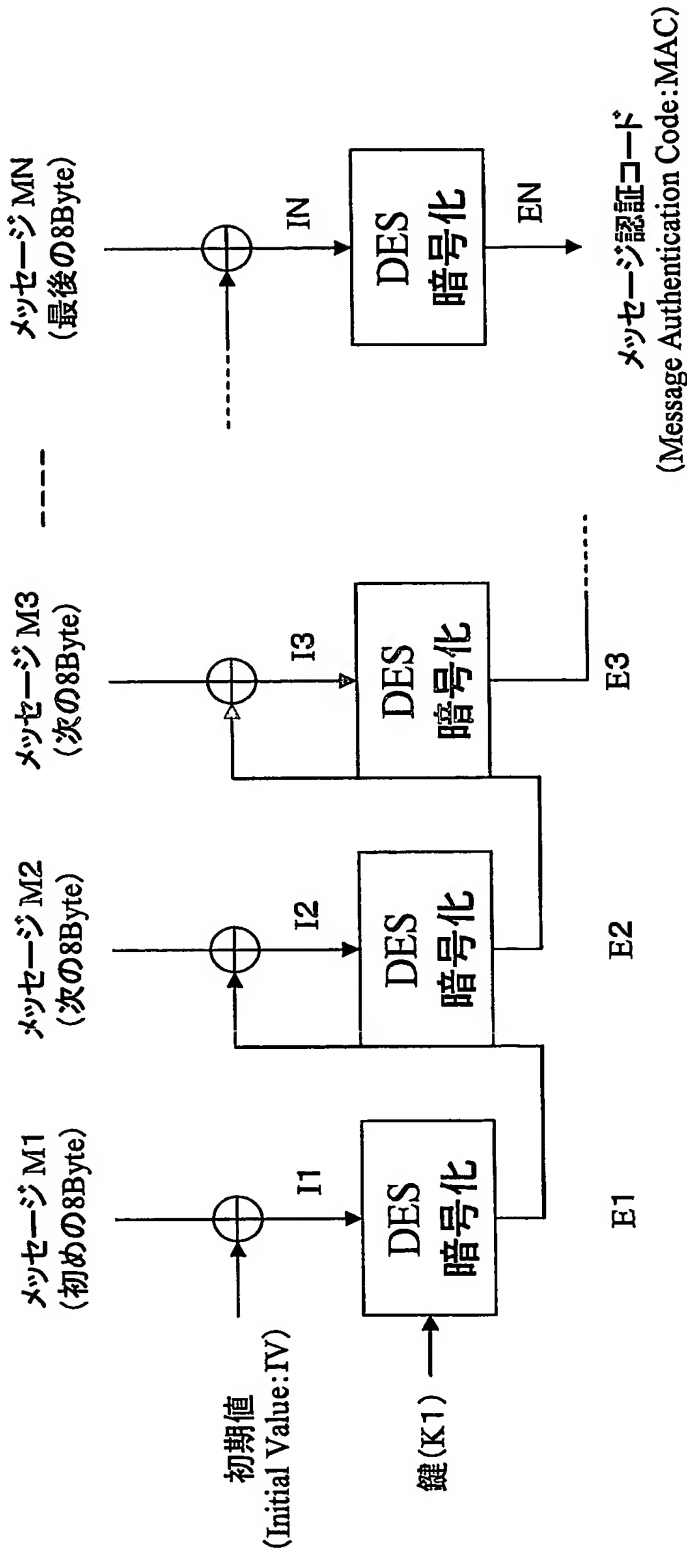


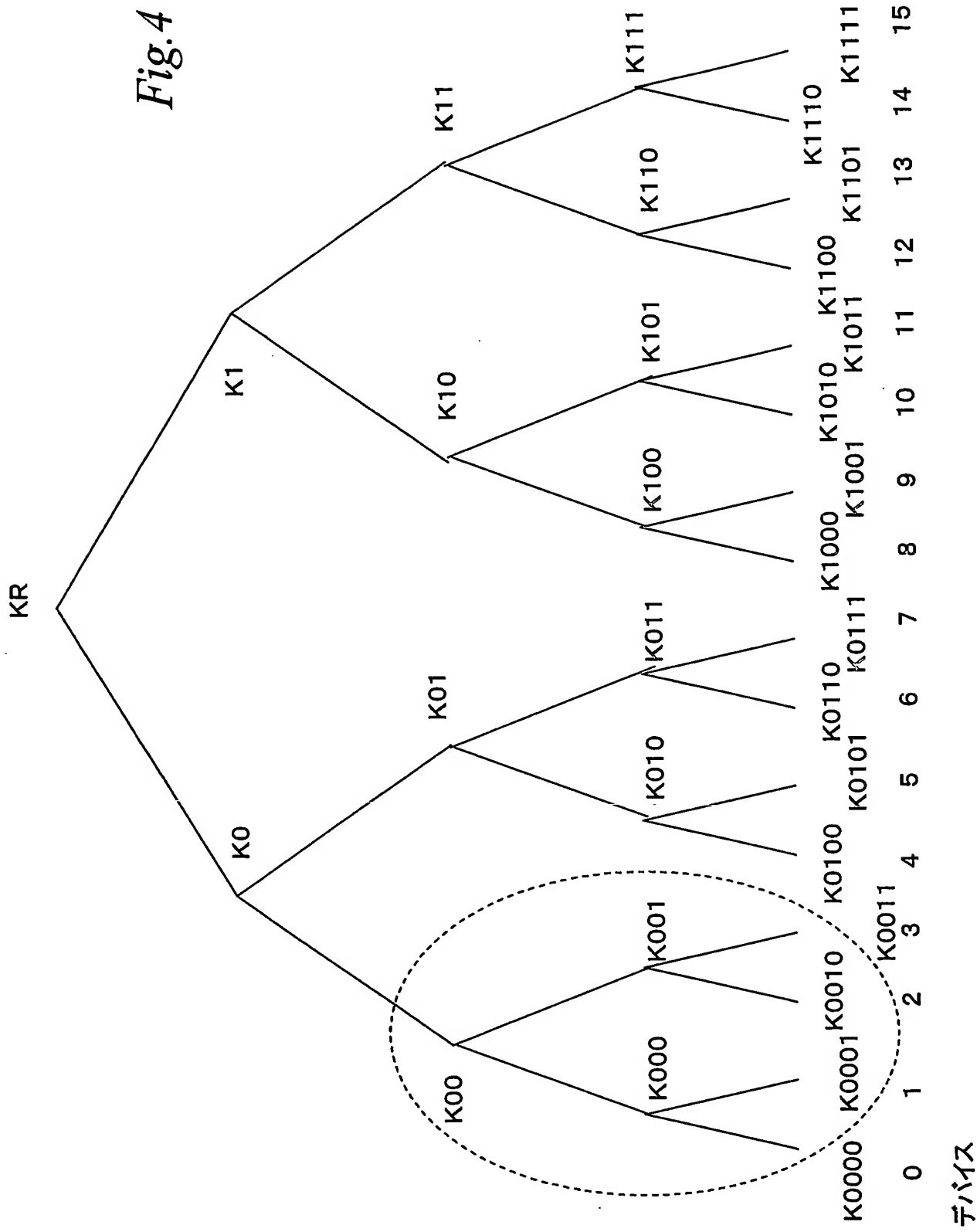
Fig. 2



\oplus : 排他的論理和処理 (8バイト単位)

Fig.3

Fig. 4



(A) 有効化キーブロック

(EKB:Enabling Key Block)例1

(B) 有効化キーブロック

(EKB:Enabling Key Block) 例2

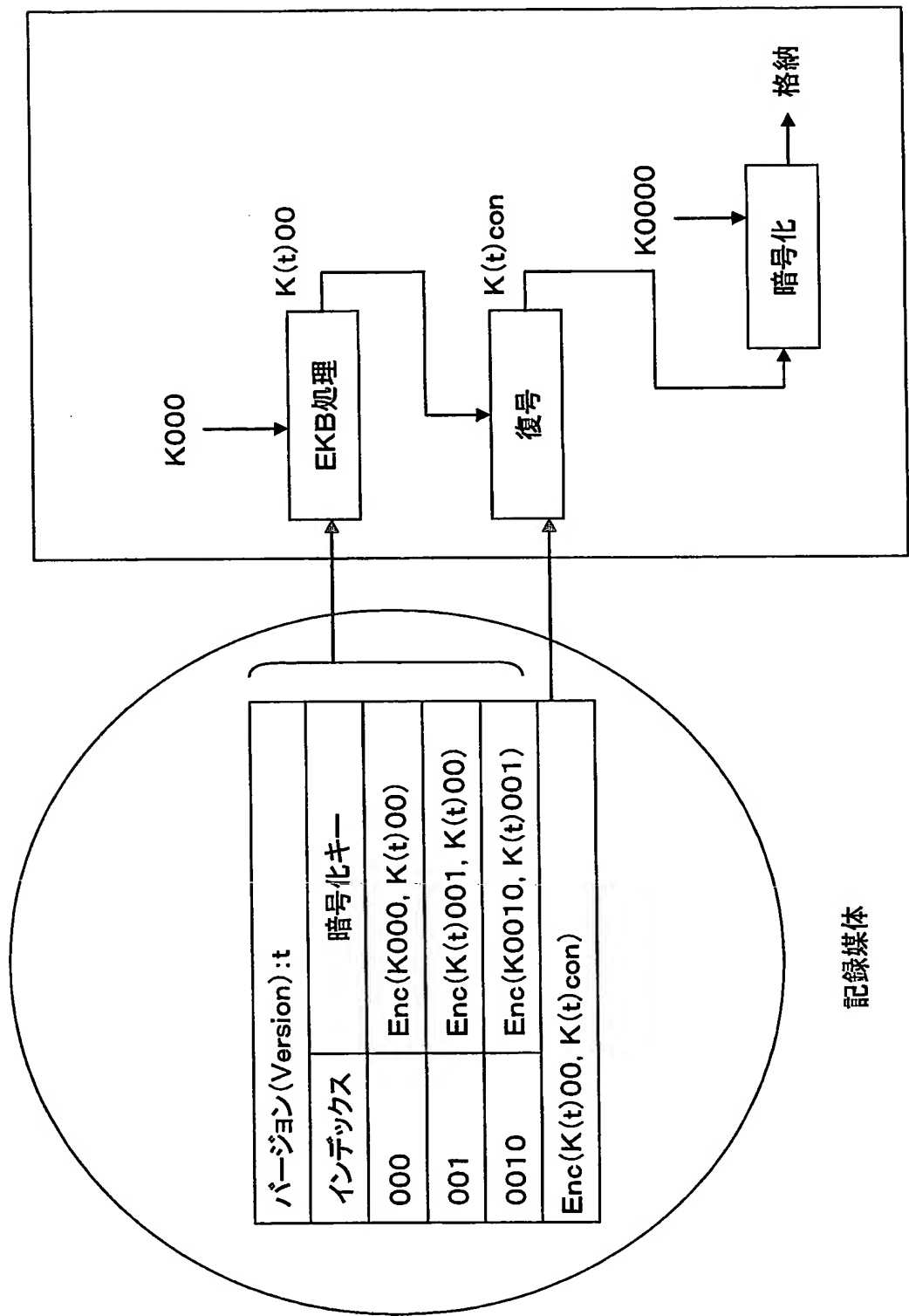
デバイス0, 1, 2にバージョン:tのノードキーを送付

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

Fig.5



デバイス0 Fig.6

201	バージョン (version)	デプス (depth)	202
203	データポインタ (Data pointer)	タグポインタ (Tag pointer)	204
205	署名ポインタ (Signature pointer)	リザーブ (reserved)	
	データ部(E(k0, Kroot), ...)		206
	タグ部({0, 0}, {1, 1}, ...)		207
	署名 (Signature)		208

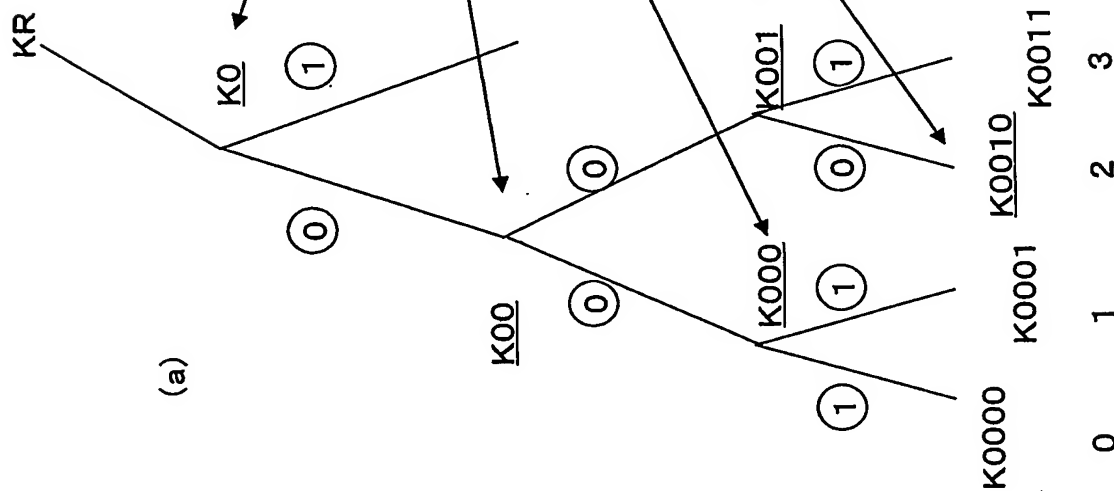
Fig. 7

Fig. 8

(१)

有効化キーブロック(EKB:Enabling Key Block)

デバイス0, 1, 2にバージョン:tのノードキーを送付



トップノードアドレス:KR	
データ(暗号化キー)	タグ
$Enc(K(t)0, K(t)R)$	$[0, 1]$
$Enc(K(t)00, K(t)0)$	$[0, 0]$
$Enc(K000, K(t)00)$	$[1, 1]$
$Enc(K(t)001, K(t)00)$	$[0, 1]$
$Enc(K0010, K(t)001)$	$[1, 1]$

{Lタグ, Rタグ}

左(L)右(R)それぞれの方向にデータがあれば0、なければ1

(c)

データ: $\text{Enc}(K(t)0, K(t)R), \text{Enc}(K(t)00, K(t)0), \dots$
 タグ : $[0, 1], [0, 0], [1, 1] \dots$

9/17

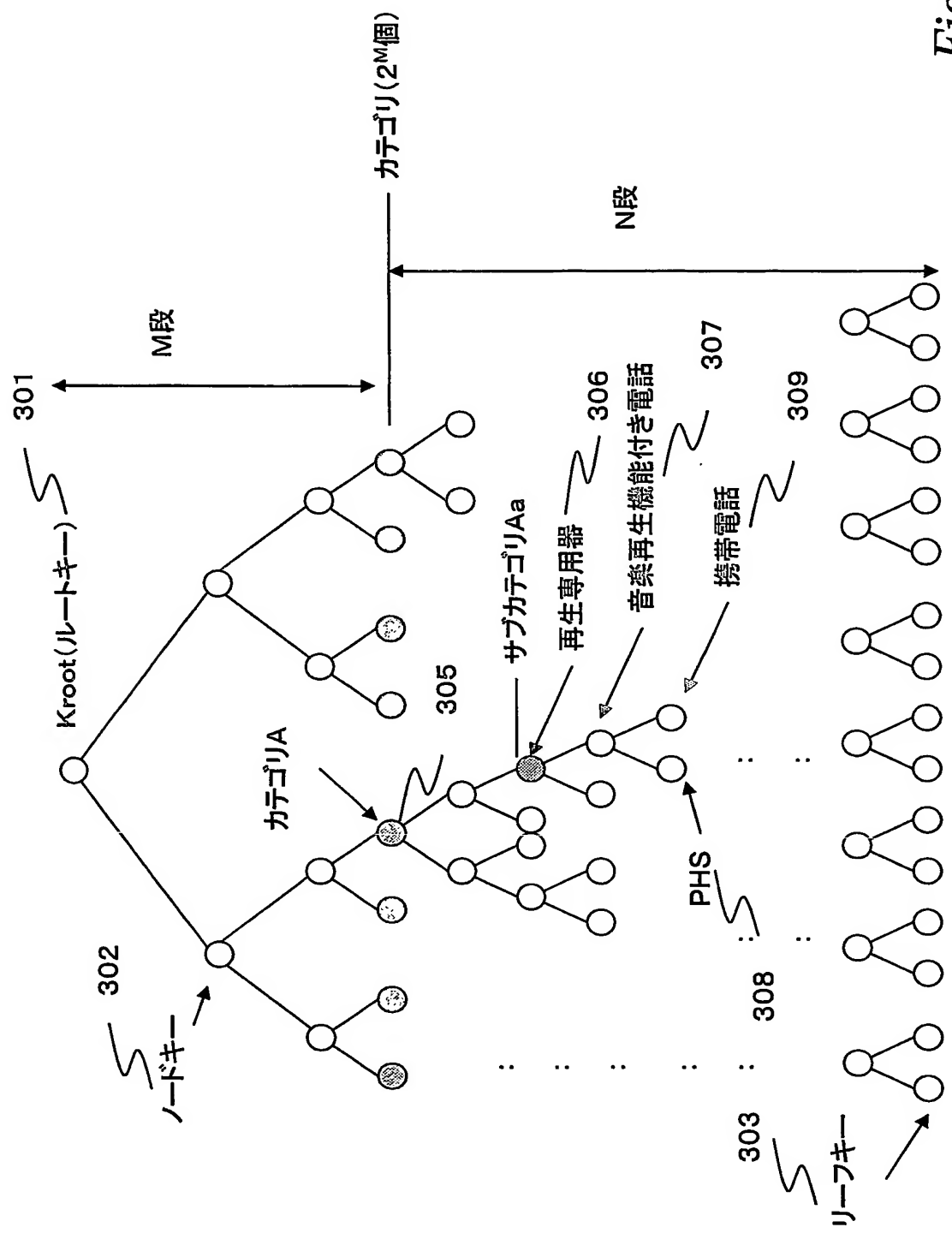


Fig.9

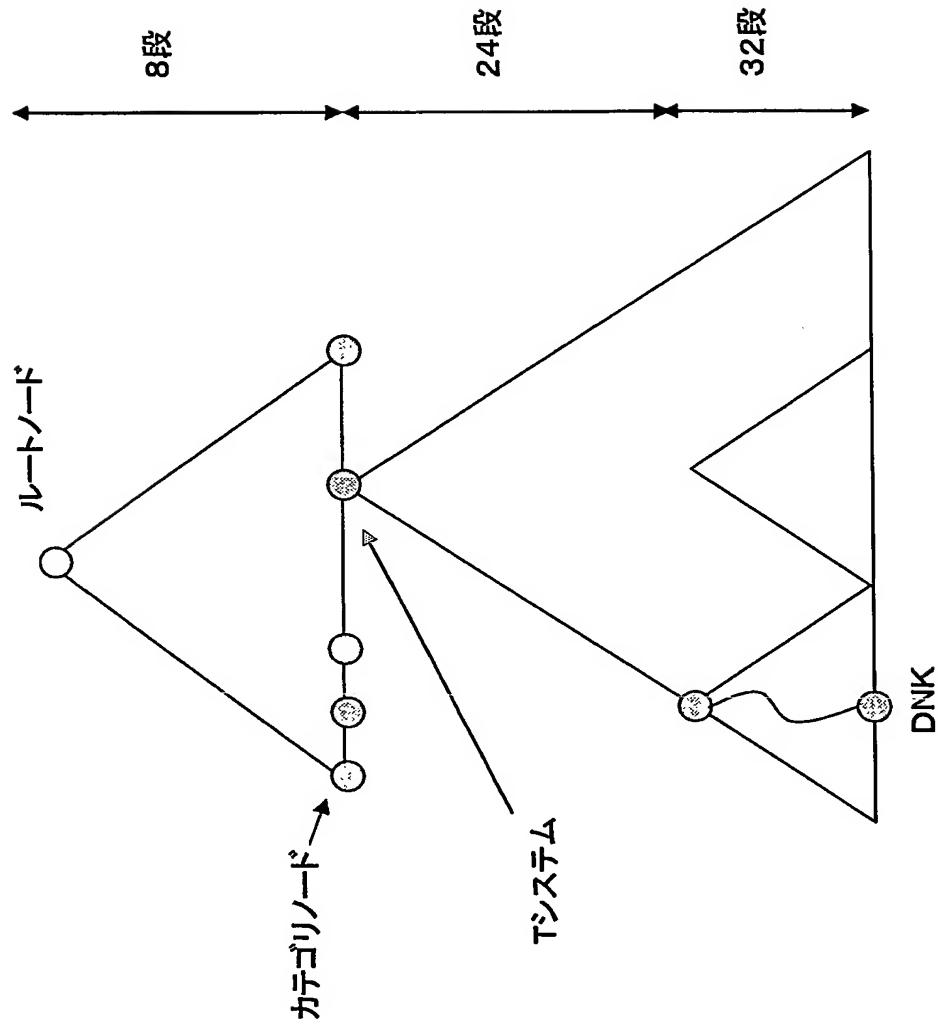


Fig.10

11/17

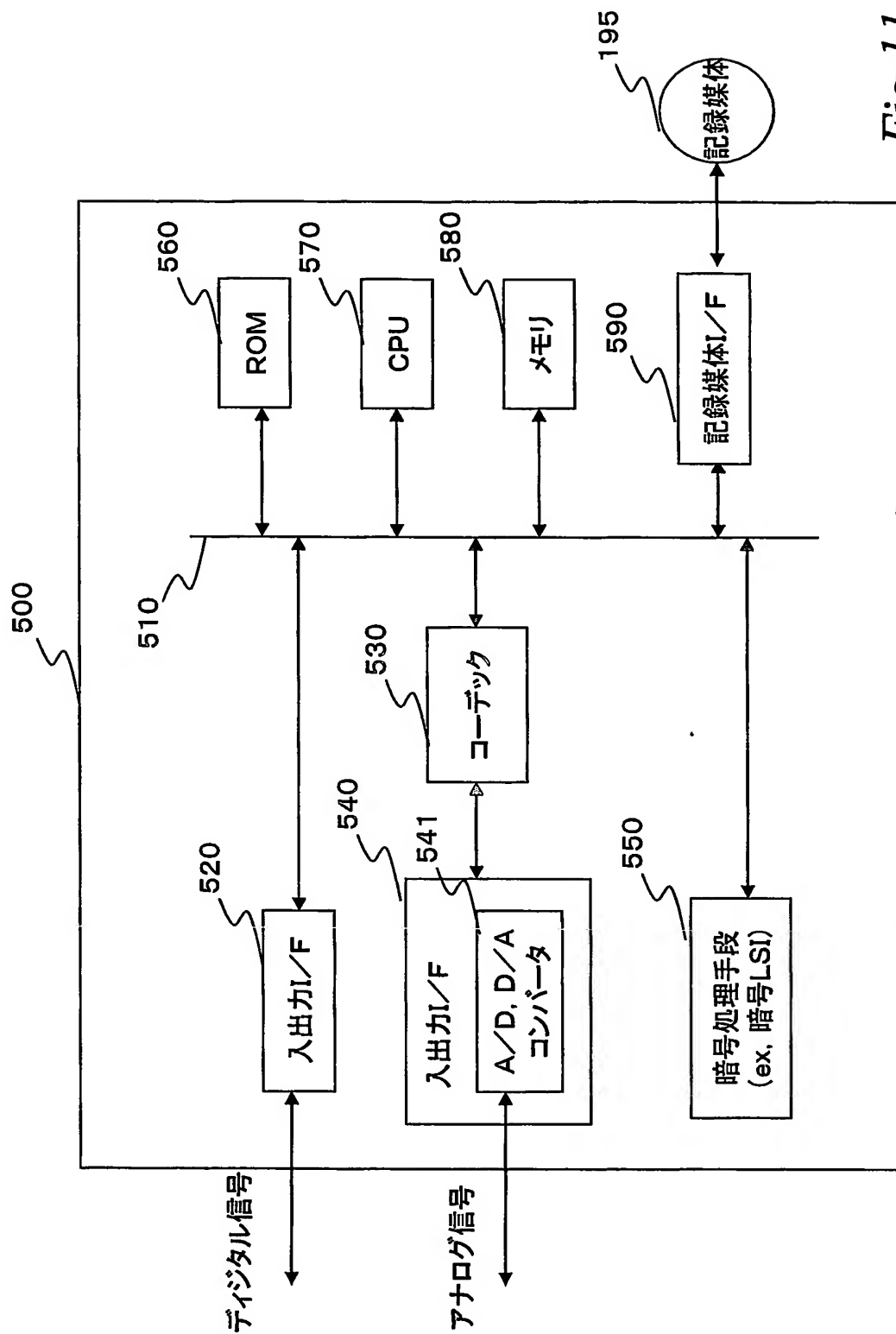


Fig. 11

12/17

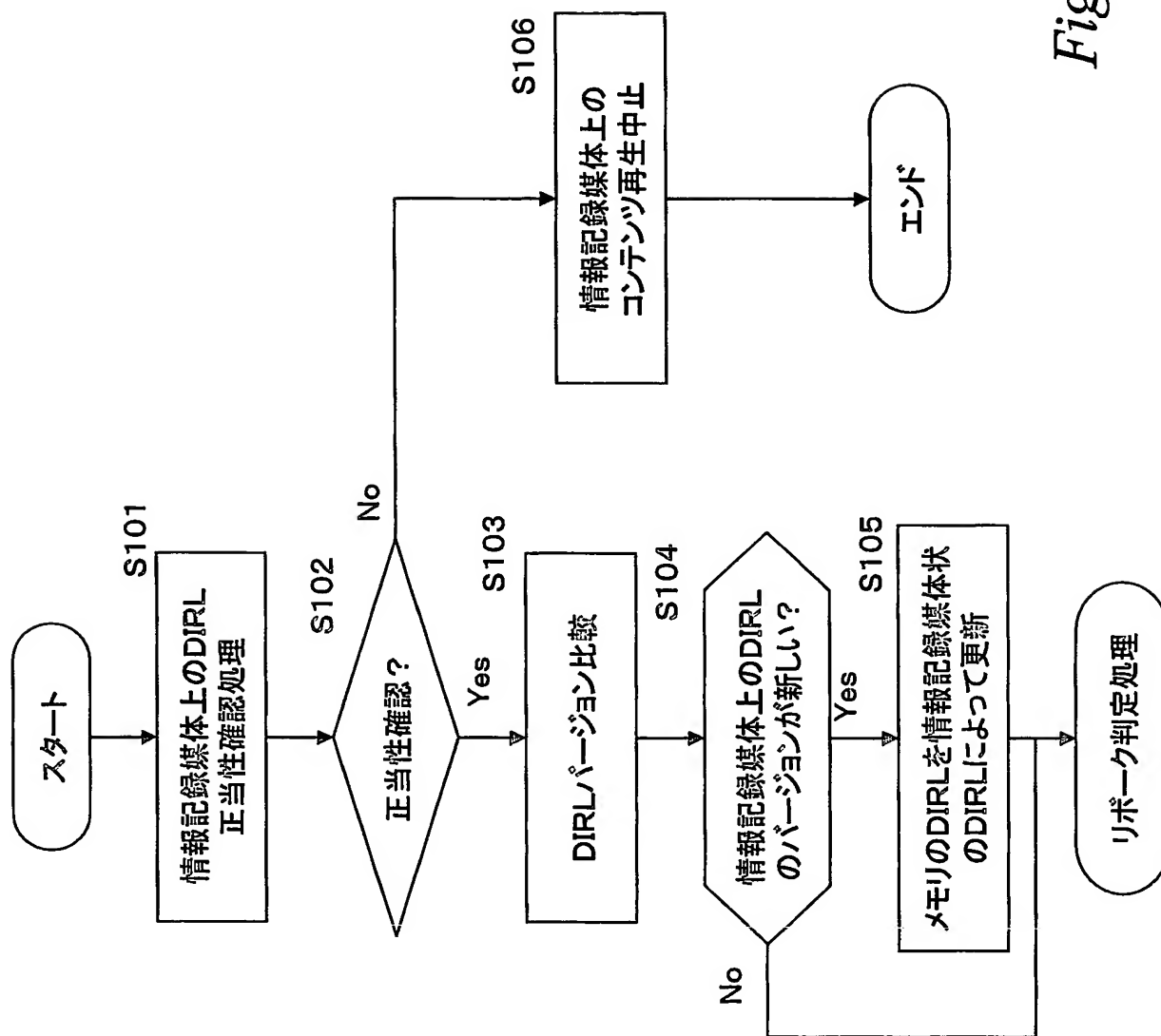


Fig. 12

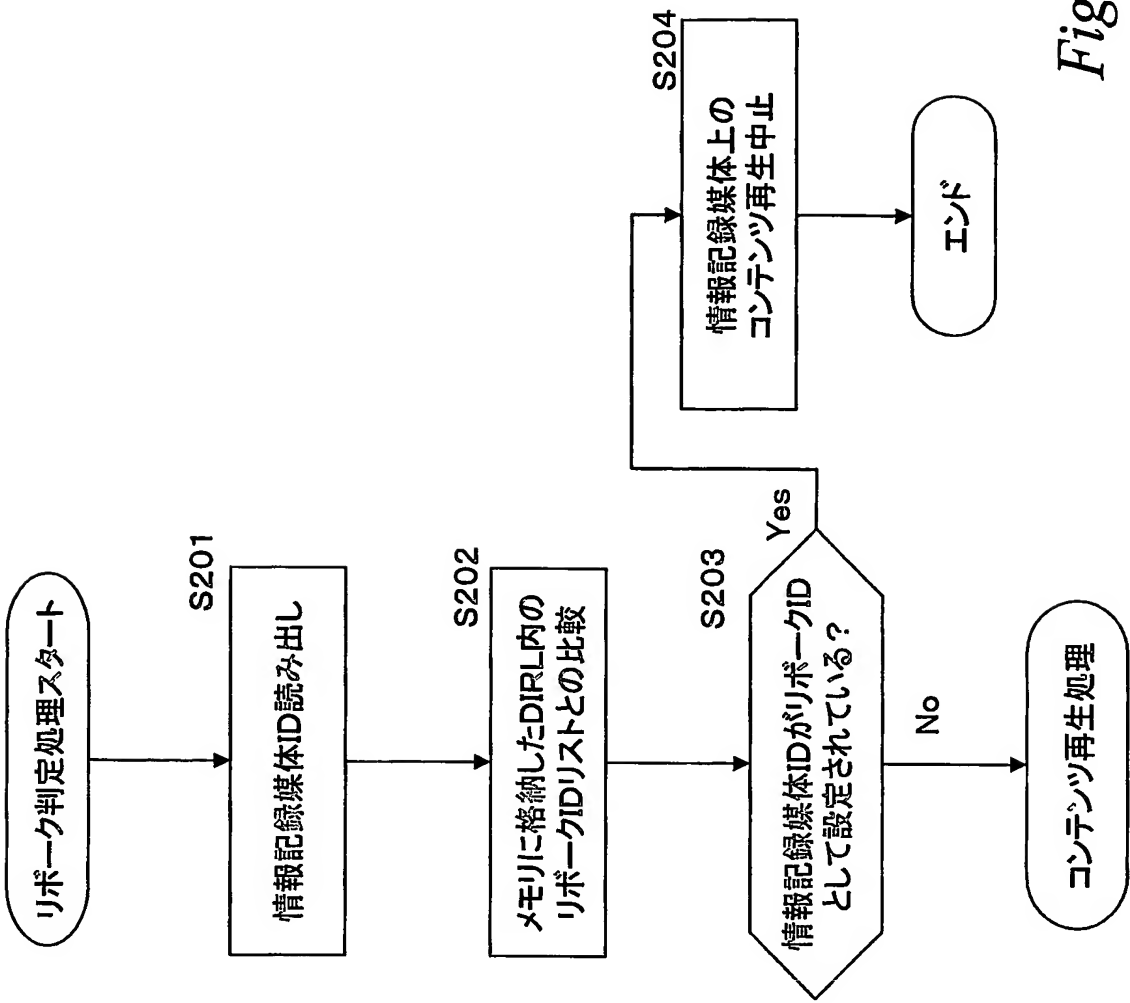


Fig. 13

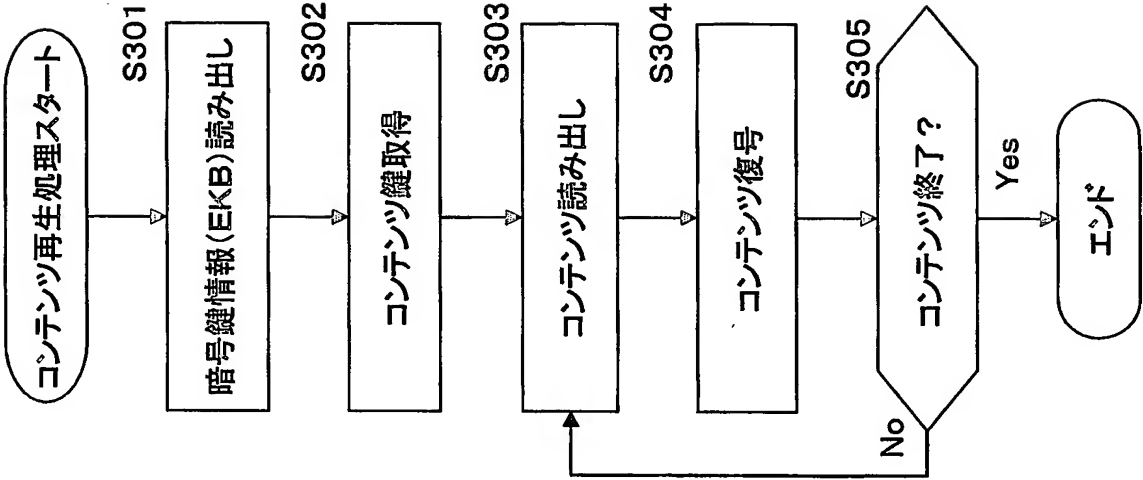


Fig.14

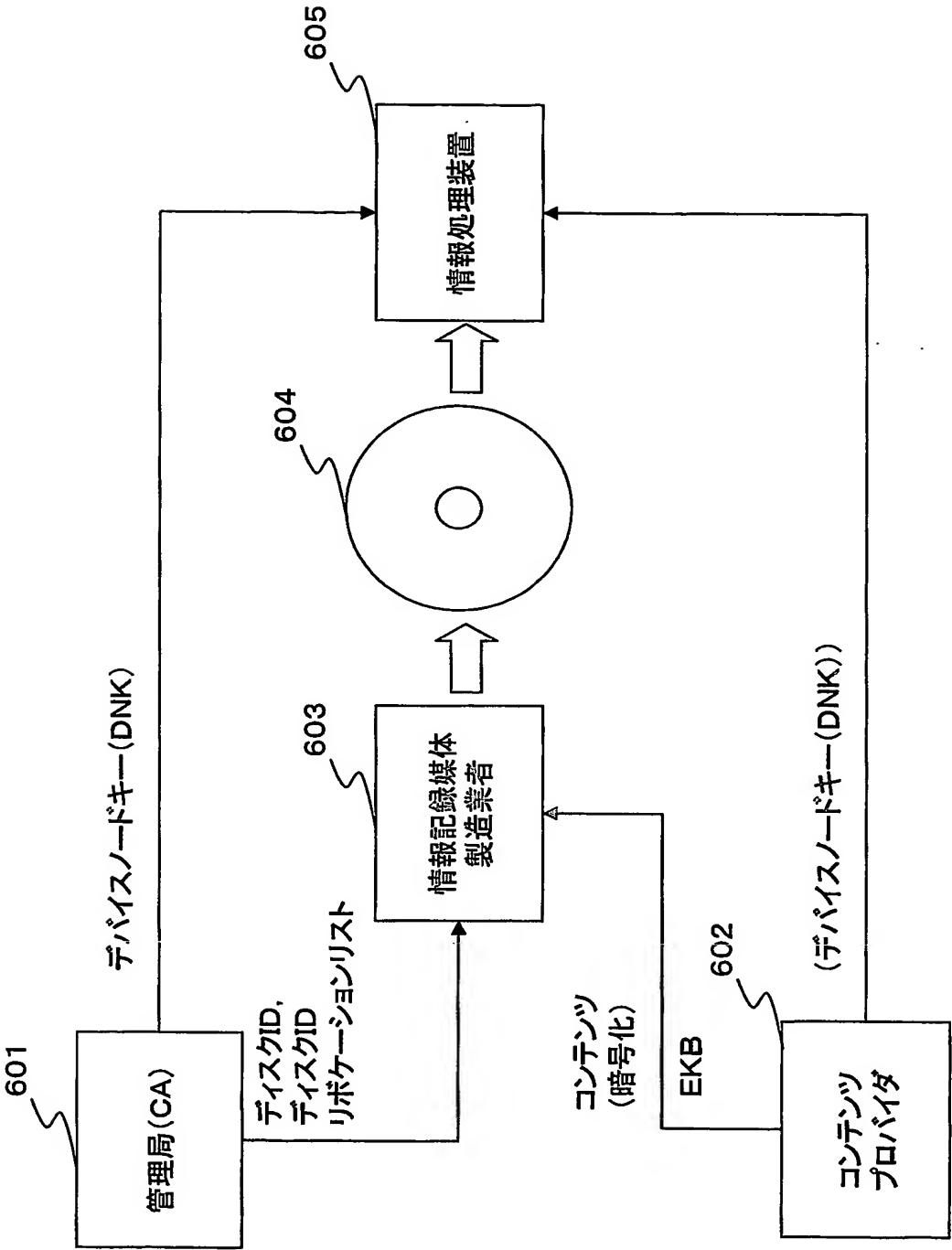


Fig. 15

16/17

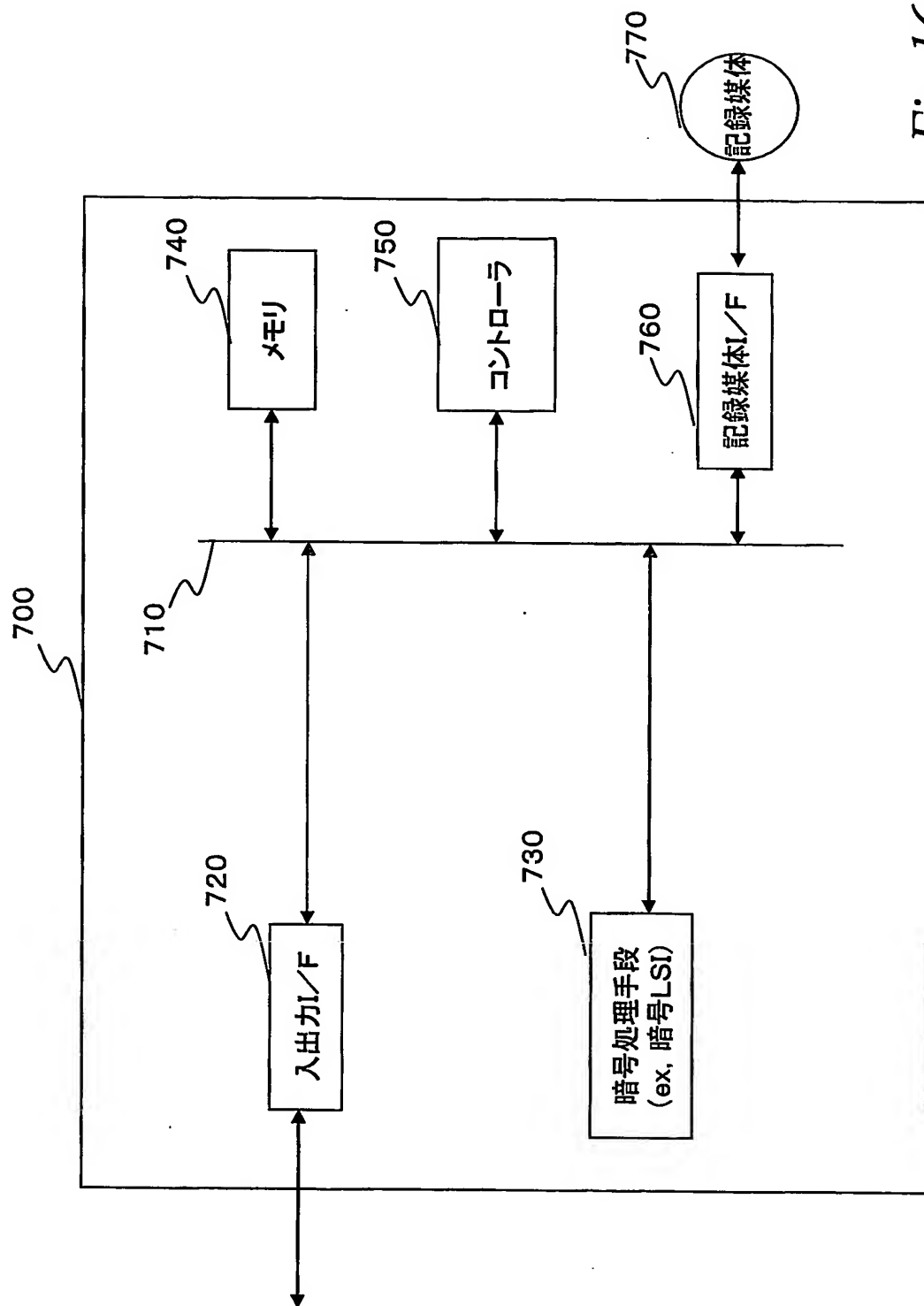


Fig. 16

17/17

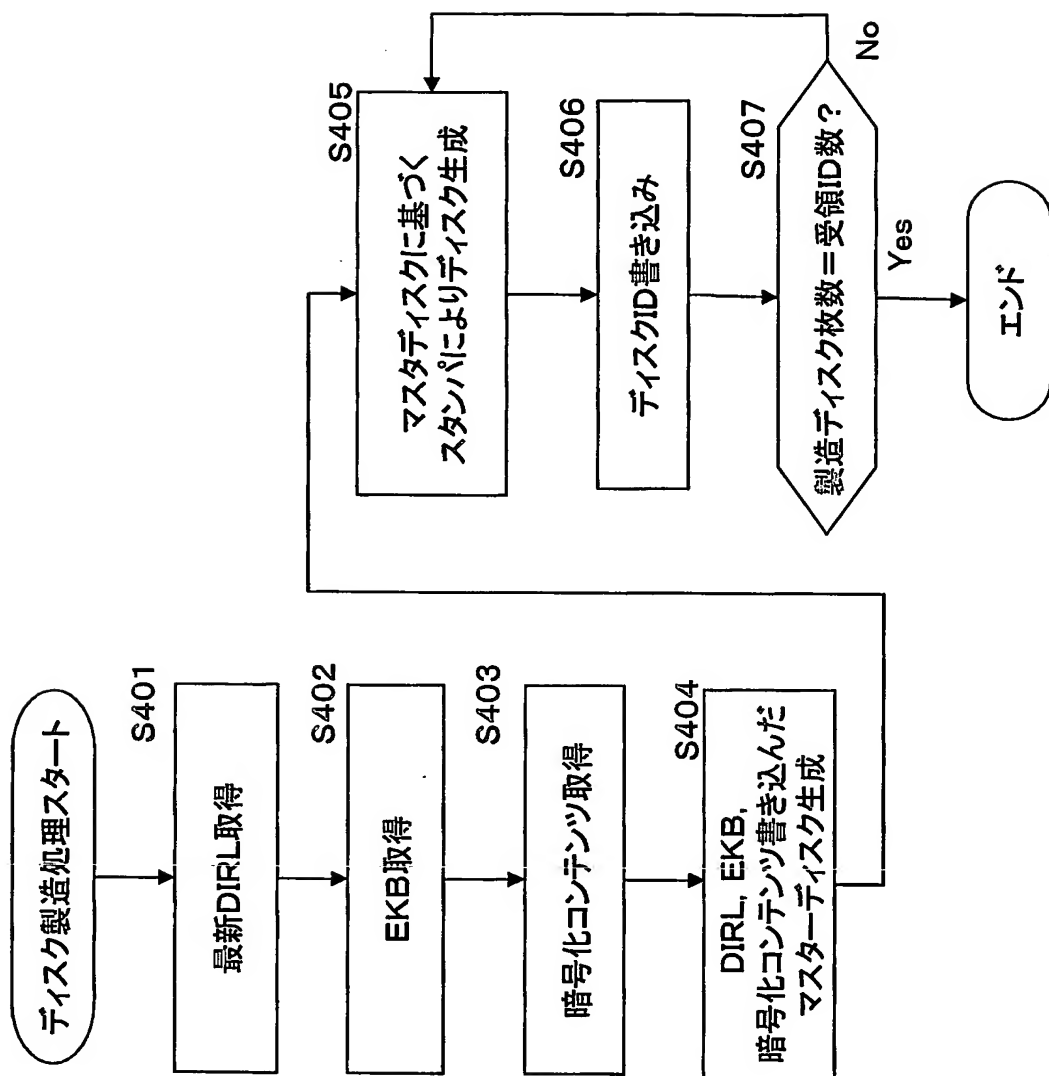


Fig.17

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/003579

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G11B20/10, H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G11B20/10, H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-256113 A (Toshiba Corp.), 21 September, 2001 (21.09.01), All pages; all drawings & US 2001/0021255 A1	5-15
A	JP 2002-133767 A (Sony Corp.), 10 May, 2002 (10.05.02), All pages; all drawings (Family: none)	5-15
A	JP 2002-237808 A (Toshiba Corp.), 23 August, 2002 (23.08.02), All pages; all drawings & US 2002/0111925 A1	5-15

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"I" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

08 June, 2004 (08.06.04)

Date of mailing of the international search report

29 June, 2004 (29.06.04)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/003579

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 1-4

because they relate to subject matter not required to be searched by this Authority, namely:

The information recording medium disclosed in claims 1-4 is characterized only by the content of the information presented and has a main object to present information recorded.

Accordingly, claims 1-4 relate to mere presentations of information.

2. ☐ Claims Nos.:

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl.⁷ G06F12/14, G11B20/10, H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl.⁷ G06F12/14, G11B20/10, H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国実用新案登録公報	1996-2004年
日本国登録実用新案公報	1994-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-256113 A (株式会社東芝) 2001.09.21, 全頁, 全図 & US 2001/0021255 A1	5-15
A	JP 2002-133767 A (ソニー株式会社) 2002.05.10, 全頁, 全図 (ファミリーなし)	5-15
A	JP 2002-237808 A (株式会社東芝) 2002.08.23, 全頁, 全図 & US 2002/0111925 A1	5-15

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

08.06.2004

国際調査報告の発送日

29.6.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
高橋 克

5N 3044

電話番号 03-3581-1101 内線 3585

第II欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求の範囲 1-4 は、この国際調査機関が調査することを要しない対象に係るものである。つまり、
請求の範囲1-4に記載された情報記録媒体は、提示される情報の内容にのみ特徴を有するものであって、記録されている情報の提示を主たる目的としている。
よって、請求の範囲1-4は、情報の単なる提示である。
2. ☐ 請求の範囲 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第III欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。